Journal of Autonomous Intelligence (2024) Volume 7 Issue 4
doi: 10.32629/jai.v7i4.1272

ORIGINAL RESEARCH ARTICLE

Correlating forensic data for enhanced network crime investigations: Techniques for packet sniffing, network forensics, and attack detection

Dhwaniket Kamble[1,2,*], Santosh Rathod[2], Manish Bhelande[3], Alok Shah[4], Pravin Sapkal[2]

[1] *G H Raisoni University, Amravati, Maharashtra 444701, India*

[2] *Department of Engineering and Technology, Bharati Vidyapeeth Deemed University, Navi Mumbai, Maharashtra 410210, India*

[3] *Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra 400088, India*

[4] *Department of Management Studies, Bharati Vidyapeeth Deemed University, Navi Mumbai, Maharashtra 410210, India*

*** Corresponding author:** Dhwaniket Kamble, sakec.dhwaniketk@gmail.com, drkamble@bvucoep.edu.in

ABSTRACT

In today's digitally saturated world, digital devices are frequently involved in criminal events as targets, mediums, or witnesses. Forensic investigations encompass the collection, recovery, analysis, and presentation of information stored on network devices, with specific relevance to network crimes. Such investigations often necessitate the use of diverse analysis tools and methods. This study introduces techniques that support digital investigators in correlating and presenting information derived from forensic data, with a primary focus on packet sniffing, network forensics, and attack detection. By leveraging these methodologies, investigators aim to achieve more valuable reconstructions of events or actions, resulting in enhanced case conclusions. The study emphasizes the importance of understanding how malware operates within the context of the Internet. It explores packet sniffing techniques to capture and analyze network data, enabling investigators to detect and trace the origins of malicious activities. Additionally, it delves into the realm of network forensics, proposing effective methods for gathering evidence from network devices and reconstructing digital events. Furthermore, the study covers the significance of attack detection in network crime investigations. It highlights techniques to identify and analyze attack patterns, facilitating the identification of perpetrators and their motivations. By correlating information obtained from forensic data, investigators can obtain comprehensive insights into the nature and impacts of network crimes. Overall, this study aims to arm digital investigators with the knowledge and tools necessary to navigate the complexities of packet sniffing, network forensics, and attack detection. By incorporating these techniques into their investigations, investigators can achieve more robust reconstructions of events, draw well-informed conclusions, and contribute to the successful resolution of network crime cases.

Keywords: network forensics; evidence; network traffic; sniffing; analysis

ARTICLE INFO

Received: 21 November 2023
Accepted: 5 December 2023
Available online: 5 February 2024

1. Introduction

Network forensics is a pivotal component in the process of scrutinizing and addressing network security incidents. It operates by amalgamating various methodologies such as network sniffing, capturing, and analysis techniques. The essence of network forensics lies in its ability to harness traffic data and event logs, empowering investigators to unveil the intricacies of network attacks and pinpoint the individuals accountable for them. The practice of network forensics is indispensable in the realm of cybersecurity, as it furnishes crucial insights into the nature and origin of security breaches. Through meticulous examination of network activities, security professionals can unravel the tactics employed by malicious actors, ultimately

facilitating the development of robust countermeasures to fortify network defenses. However, despite its significance, the execution of effective network forensics is not without its challenges. The complexities arise from a myriad of factors that necessitate meticulous consideration. The sheer volume of data generated in a network environment poses a formidable obstacle, requiring investigators to sift through vast amounts of information to discern relevant patterns and anomalies. Additionally, the dynamic nature of network environments, characterized by constant changes and updates, further complicates the forensic process. Furthermore, the diverse array of devices, protocols, and applications within a network introduces intricacies that demand a nuanced understanding. Interpreting the intricacies of encrypted communication, identifying false positives, and overcoming obfuscation techniques employed by sophisticated attackers are among the hurdles that network forensics practitioners encounter. While network forensics is an invaluable tool in the investigation and mitigation of network security incidents, its effectiveness hinges on the adept navigation of various challenges. As technology evolves, so do the methods employed by cyber adversaries, necessitating a continuous refinement of network forensics strategies to uphold the integrity and security of digital infrastructures.

One of the primary challenges in network forensics is the practical implementation of network traffic capture. Although the theoretical concept of capturing network traffic may be simple, the complexity arises due to factors like the high volume of data and the intricate nature of Internet protocols[1]. As a result, significant resources are often required to record network traffic. However, capturing all transmitted data is not always feasible due to the sheer volume of information, necessitating selective data backup for later examination. In addition to capturing network traffic, analyzing the recorded data is a time-consuming task. While automated analysis tools exist, accurately differentiating malicious traffic from legitimate traffic remains challenging. The reliance on human judgment is crucial to mitigate false positive results. This highlights the importance of proactively establishing robust event recording and data collection systems to ensure preparedness for network forensics[2]. These systems enable the availability of vital artifacts for examination during forensic inquiries. This paper aims to address the challenges posed by network forensics, specifically focusing on the capture, analysis, and admissibility of evidence. By exploring techniques, methodologies, and best practices, this research contributes to the enhancement of network forensics capabilities. The primary goal is to improve the ability of investigators to effectively and efficiently capture and analyze network traffic, enhance the accuracy of distinguishing malicious activities, and ensure the admissibility of evidence in a legal context. Through this research, we seek to provide insights and recommendations that empower digital investigators to overcome the challenges associated with network forensics. By doing so, we can contribute to the field's advancements and facilitate the successful resolution of network security incidents.

2. Materials and methods/methodology

In the contemporary digital landscape, where technology pervades every aspect of daily life, criminal activities are increasingly entwined with digital devices, assuming roles as targets, mediums, or even witnesses in illicit events. This necessitates the evolution of forensic practices to encompass the intricate processes of collecting, recovering, analyzing, and presenting information stored on network devices, with a specific emphasis on addressing the challenges posed by network crimes. This literature review explores the diverse array of tools and methodologies available to digital investigators, focusing primarily on packet sniffing, network forensics, and attack detection, to enhance the reconstruction and resolution of network crime cases. The study commences by underscoring the critical role of understanding the operation of malware within the expansive realm of the Internet. A pivotal aspect of this understanding involves the utilization of packet sniffing techniques, which enable the comprehensive capture and analysis of network data. By leveraging these techniques, investigators can unveil the origins of malicious activities, facilitating the tracing and identification

of digital adversaries. This emphasis on packet sniffing underscores its significance as a foundational step in digital investigations, providing valuable insights into the tactics employed by perpetrators. Moving forward, the literature review delves into the intricacies of network forensics, presenting effective methodologies for the systematic gathering of evidence from network devices. This includes the reconstruction of digital events, enhancing investigators' capacity to build a cohesive narrative around criminal activities. The study acknowledges the dynamic nature of network environments and proposes adaptive strategies to navigate challenges such as encrypted communication, false positives, and obfuscation techniques employed by sophisticated adversaries. Furthermore, the review addresses the pivotal aspect of attack detection in the context of network crime investigations. It sheds light on advanced techniques for identifying and analyzing attack patterns, thereby aiding investigators in the identification of perpetrators and the understanding of their motivations. This section emphasizes the proactive stance of digital investigators in anticipating, identifying, and mitigating potential threats within network infrastructures. A recurring theme throughout the literature review is the integration and correlation of information derived from forensic data. By combining insights from packet sniffing, network forensics, and attack detection, investigators can construct a comprehensive understanding of the nature and impacts of network crimes. This holistic approach positions digital investigators to draw well-informed conclusions, contributing significantly to the successful resolution of network crime cases.

This comprehensive review aims to equip digital investigators with the knowledge and tools essential for navigating the complexities of packet sniffing, network forensics, and attack detection. Through the incorporation of these advanced techniques into their investigative processes, practitioners can enhance the robustness of event reconstructions, make informed conclusions, and ultimately contribute to the successful resolution of network crime cases in the digitally saturated world of today. Consider incorporating instances where the outlined techniques were successfully employed, showcasing how packet sniffing, network forensics, and attack detection contributed to the resolution of actual cases.

2.1. Collecting evidence

The process of locating and collecting data, which is often distributed across network devices and traffic paths within a network, plays a vital role in investigating incidents. This data gathering becomes crucial when facing external threats attempting to compromise internal systems or extract information from the network. Network-based evidence is especially valuable when assessing host evidence, as it serves as a secondary source of event confirmation, greatly aiding in the identification of the root cause behind an incident.

2.1.1. Sniffers

The information flow within a network can provide valuable insights into intrusions or unusual connections. Packet sniffers, also known as network sniffers, have been developed to address the need for capturing this data[3]. By placing network interface cards (NICs) in promiscuous mode, sniffers are able to intercept and record all network traffic. Switched networks can be facilitated for sniffing through the use of hardware taps and spanned ports. Sniffers not only capture data at the physical and data-link layers but also extend their capabilities to the network and transport layers. These packet sniffers play a crucial role in network forensics by enabling traffic management, monitoring network components, and detecting security breaches. Forensic investigators utilize sniffers to scrutinize any suspicious applications or devices, leveraging their monitoring and analysis functionalities.

A few examples of sniffers are as follows:

1) Sniffing tool: Tcpdump

Tcpdump is a tool that, when a Boolean input expression aligns with a packet on a network interface, displays a description of the packet's contents. By utilizing the -w parameter, the program can save the packet data to a file for later analysis, while the -r flag enables the program to read packets from a stored packet file

instead of a network interface[4]. Tcpdump exclusively examines packets that precisely match the provided expression. When Tcpdump is executed without the -c flag, it captures packets until it receives a SIGINT or SIGTERM signal, or until the specified number of packets has been processed. However, when the -c flag is used, it captures packets until it receives a SIGINT or SIGTERM signal or until the specified number of packets has been processed.

2) Sniffing tool: Wireshark

Wireshark stands out as a powerful and versatile graphical user interface (GUI) network protocol analyzer (**Figure 1**), serving as a crucial tool for investigators engaged in digital forensics and network analysis. The application provides investigators with an interactive platform, allowing them to examine packet data from live networks or previously captured files. This capability enables forensic experts to gain profound insights into the intricacies of network communication, aiding in the identification and analysis of potential security incidents[5]. One of Wireshark's notable features is its utilization of the libpcap format as its native capture file format. This format is widely supported across various network analysis utilities, including tcpdump, establishing compatibility and interoperability within the digital forensics ecosystem. This standardized approach facilitates seamless collaboration among different tools, ensuring a cohesive and comprehensive analysis of network traffic data. Wireshark's versatility is further underscored by its ability to conduct both real-time capture and offline analysis. In real-time mode, investigators can monitor and capture data as it flows through the network, allowing for immediate response to ongoing incidents[6]. Simultaneously, the tool supports the examination of previously captured files, enabling thorough retrospective analysis of historical network activity. This dual functionality equips investigators with the flexibility to address diverse investigative scenarios. Another noteworthy aspect of Wireshark is its broad compatibility with multiple operating systems, including Windows OS, Linux, macOS, Solaris, FreeBSD, and NetBSD. This cross-platform support enhances the accessibility and applicability of Wireshark across various environments, catering to the diverse preferences and requirements of digital investigators. Wireshark's adeptness extends to its capability to read gzip-compressed file types without the need for a .gz extension. This feature streamlines the analysis process by directly recognizing and interpreting compressed files, demonstrating Wireshark's commitment to user convenience. The main window of Wireshark provides investigators with a comprehensive view of each packet, presenting information through three distinct perspectives. The summary line offers a quick overview of key packet details, facilitating rapid initial assessments. The protocol tree, on the other hand, allows for in-depth exploration of specific protocols or topics, enabling investigators to drill down into the nuances of network communication. Additionally, the hex dump view illustrates the raw hexadecimal representation of the packet, offering a granular perspective on the packet's structure and content during transmission[7]. In essence, Wireshark emerges as a sophisticated and user-friendly network protocol analyzer, adeptly balancing real-time and offline analysis capabilities. Its compatibility with various operating systems and support for common file formats, along with its intuitive interface featuring multiple packet views, positions Wireshark as an invaluable tool in the arsenal of digital investigators seeking to unravel the complexities of network communication and enhance their forensic analyses.

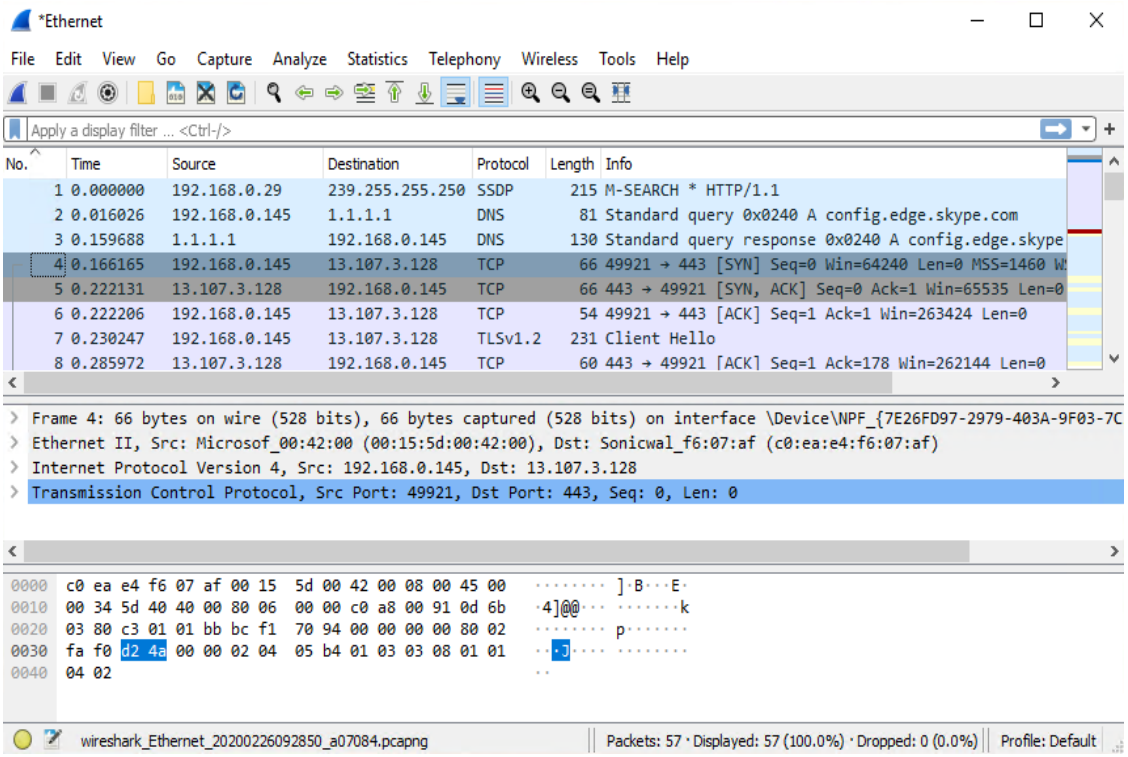

Figure 1. Wireshark graphical user interface (GUI) network protocol analyzer.

2.1.2. Security Information and Event Management System (SIEM)

Many companies face the challenge of limited access to network device logs due to log file rollover, where new logs overwrite previous ones due to space constraints. This can result in organizations having only a few days or even a few hours' worth of critical logs, leaving the incident response team without crucial evidence for events that occurred weeks earlier[8]. To address this issue, the Security Information and Event Management (SIEM). System has gained popularity as an enterprise-wide technology. These systems are capable of collecting log and event information from multiple network sources and consolidating it in one central location, eliminating the need to examine individual systems and enabling comprehensive network activity monitoring by the CSIRT and security experts[9]. By sending logs from various sources such as SQL databases and security controls to an SIEM system, suspicious activities like the use of a user account to copy a database to a remote server can be quickly identified and investigated[10,11]. With an SIEM system, CSIRT analysts can instantly search for any activity associated with a compromised account and access the corresponding log records, saving valuable time compared to manually searching through each accessed system in the absence of an SIEM system.

2.2. Analyzing evidence

During this step, we examine the gathered information from the previous phase utilizing various tools and techniques to convert the available data into compelling evidence that helps address the fundamental "W questions": what, when, why, where, and how[12]. This stage enables us to gain a comprehensive understanding of the case and explore potential motives that may have influenced the incident. Additionally, it becomes possible to accurately determine the nature of the case, whether it is unintentional, related to a dissatisfied employee, or potentially involving industrial espionage.

2.2.1. Analyzing traffic for sniffing attempts

In techniques such as sniffing and man-in-the-middle attacks, malicious individuals position themselves between a client and a server to intercept messages. By eavesdropping on network traffic, these attackers search for sensitive information.

2.2.2. Analyze traffic for MAC flooding attempt

Using the active sniffing technique called MAC flooding (**Figure 2**), the attacker connects to a port on the switch and floods it with a barrage of Ethernet transmissions containing fake MAC addresses. The objective is to overwhelm the switch's CAM (content addressable memory) table[13]. This attack is also known as a CAM flooding attack. Wireshark identifies MAC flooded packets as faulty and an investigator can utilize Wireshark's source and destination addresses, as well as the packet's time to live (TTL), to detect a MAC flooding attempt. By accessing the Analyze Expert Information tab and examining the corrupted packets, the investigator can identify signs of MAC flooding[14].

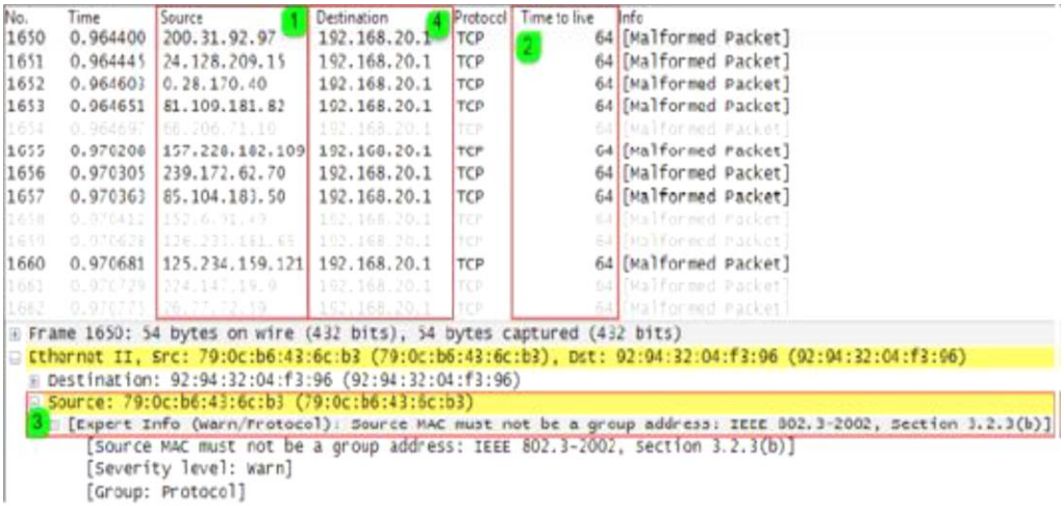

Figure 2. MAC flooding attempt.

2.2.3. Analyze traffic for SMB password cracking attempts

During the process of attempting to crack an SMB password, Wireshark's analysis of network traffic reveals multiple login attempts with different identities. The captured data indicates numerous SMB login attempts originating from Source IP 10.10.10.11 towards the Target Host (2) located at IP 10.10.10.16. The intercepted information obtained by Wireshark strongly suggests a brute-force attack targeting the SMB protocol, as evidenced by the presence of multiple usernames and the error message "Error: STATUS LOGON FAILURE".

2.2.4. Analyze traffic for TCP SYN Flood DoS Attack

SYN flooding is a type of Denial-of-Service (DoS) attack where the attacker employs numerous fabricated IP addresses to flood the target server with a massive influx of SYN packets continuously[15]. Upon receiving the SYN packets, the server responds with SYN-ACK packets, expecting an ACK packet from the client to complete the three-way TCP handshake. However, in a SYN flooding attack, the ACK packet is not received, leaving the connection incomplete[16]. As a result, the attacker can rapidly exhaust the CPU and RAM resources of the target server, rendering it unresponsive and ultimately causing a DoS situation.

2.2.5. Analyze traffic for SYN-FIN Flood DoS Attack

The SYN flag initiates a connection, while the FIN flag terminates it. In a SYN/FIN Denial-of-Service (DoS) attempt, the attacker overwhelms the network by setting both the SYN and FIN flags simultaneously[17]. It is uncommon for the SYN and FIN flags to be set together in a typical TCP conversation. If an administrator detects traffic with both the SYN and FIN flags set, it indicates a possible SYN/FIN DDoS attack. During such an attack, the continuous delivery of packets with SYN/FIN flags can overload the server's firewall, leading to potential disruptions or service unavailability.

2.2.6. Analyze traffic for FTP password cracking attempts

Password cracking refers to the process of obtaining or recovering passwords through either a password guessing attempt using a file containing commonly used passwords, or by employing trial and error methods[18]. These techniques are commonly known as dictionary attacks and brute force attacks, respectively. Detectives can identify such attacks by monitoring the number of login attempts made from the same IP address or username.

The File Transfer Protocol (FTP) is a widely utilized protocol for transferring files between computers over the Internet, using the TCP/IP suite. It operates as a client-server protocol, establishing two channels of communication between a client and server. One channel manages the discussions, while the other handles the actual transmission of data[19]. When a client requests a file download, the server responds by providing the requested file. To initiate an FTP session, the user must authenticate themselves by entering their username and password. An FTP password assault involves an attacker attempting to uncover the password of any authorized user. The motivation behind an FTP password assault can vary, ranging from unauthorized access to confidential files to potential data breaches. To mitigate the risks associated with such attacks, it is crucial for users and administrators to implement strong password policies, incorporating complex and unique combinations of characters, and to regularly monitor and audit FTP server logs for any signs of suspicious or unauthorized access attempts. Additionally, employing encryption mechanisms such as FTPS (FTP Secure) or SFTP (Secure File Transfer Protocol) enhances the security of FTP transactions, safeguarding sensitive information during file transfers over the network.

The process of analyzing FTP (File Transfer Protocol) login attempts (**Figure 3**), is a critical aspect of network security and digital forensics. In this context, the statement suggests a specific methodology for examining successful FTP login activities using a network protocol analyzer like Wireshark. The command "ftp.response.code == 230" (**Figure 4**), is a filter that can be applied within Wireshark to selectively view only those packets related to FTP responses with the code 230.

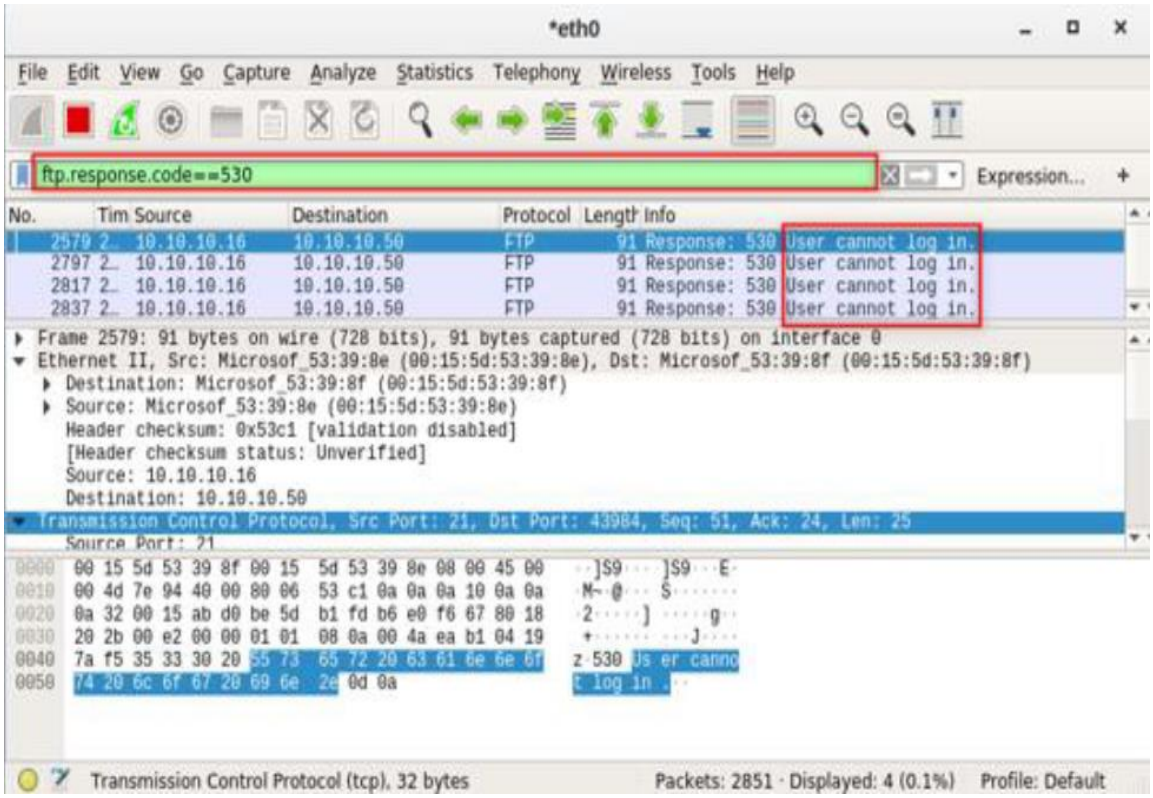

Figure 3. Analysis of all successful FTP login attempts.

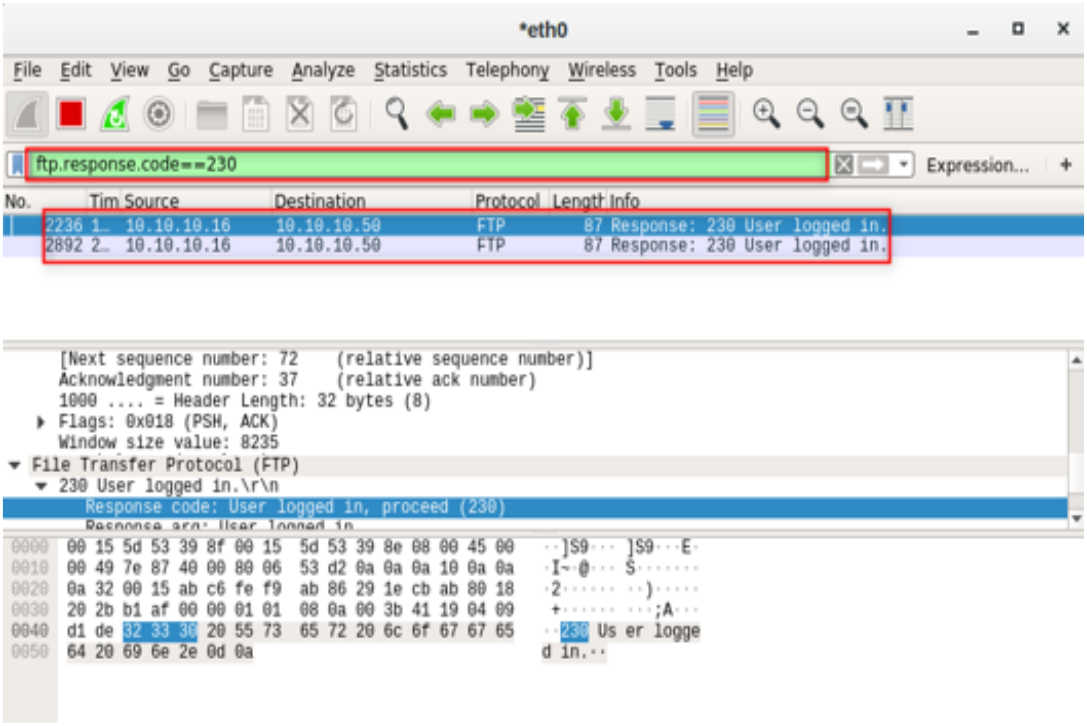

Figure 4. Applying the filter ftp.response.code == 230.

In the FTP protocol, the response code 230 signifies a successful login or authentication. When a user successfully logs in to an FTP server, the server responds with a message containing this specific code, indicating that the user has been authenticated and is granted access. The provided snapshot, presumably captured using Wireshark or a similar tool, is referenced to illustrate this analysis. In this snapshot, the filter has been applied, narrowing down the displayed packets to those specifically related to FTP responses with the code 230. As a result, the investigator can focus on instances where successful logins have occurred. The mentioned source IP address, 10.10.10.16, is highlighted as the origin of these successful login attempts. This IP address corresponds to the entity or system that initiated the FTP connection and successfully provided the correct credentials to access the FTP server.

The implication is that an attacker, represented by the mentioned IP address, was able to acquire and use valid credentials, gaining unauthorized access to the FTP server. This analysis is significant in the context of network security investigations and digital forensics. It provides concrete evidence of unauthorized access to an FTP server by pinpointing specific instances of successful logins. Such findings can be crucial in understanding the scope and impact of a security incident, determining the extent of unauthorized access, and aiding in the identification of potential security vulnerabilities.

To respond effectively to such security breaches, organizations typically take actions such as revoking compromised credentials, implementing additional security measures, and conducting a thorough investigation to understand how the unauthorized access occurred. The use of network protocol analyzers and specific filters, as described, enhances the investigator's ability to identify and respond to security incidents promptly and with precision.

2.2.7. Analyze traffic for ARP poisoning attempt

The attacker employs the active sniffing technique called MAC flooding by connecting to a port on the switch. They send a large number of Ethernet transmissions with fake MAC addresses. The objective of the attacker is to gain access to the switch's CAM (content addressable memory) table, which makes this attack also known as CAM flooding. When Wireshark detects duplicate IP addresses on the ARP protocol, it displays

a warning message stating “multiple usage of IP address detected”[20]. To identify signs of an ARP poisoning attack (**Figure 5**), you can collect the packets and apply the filter “arp.duplicate-address-detected” for analysis.

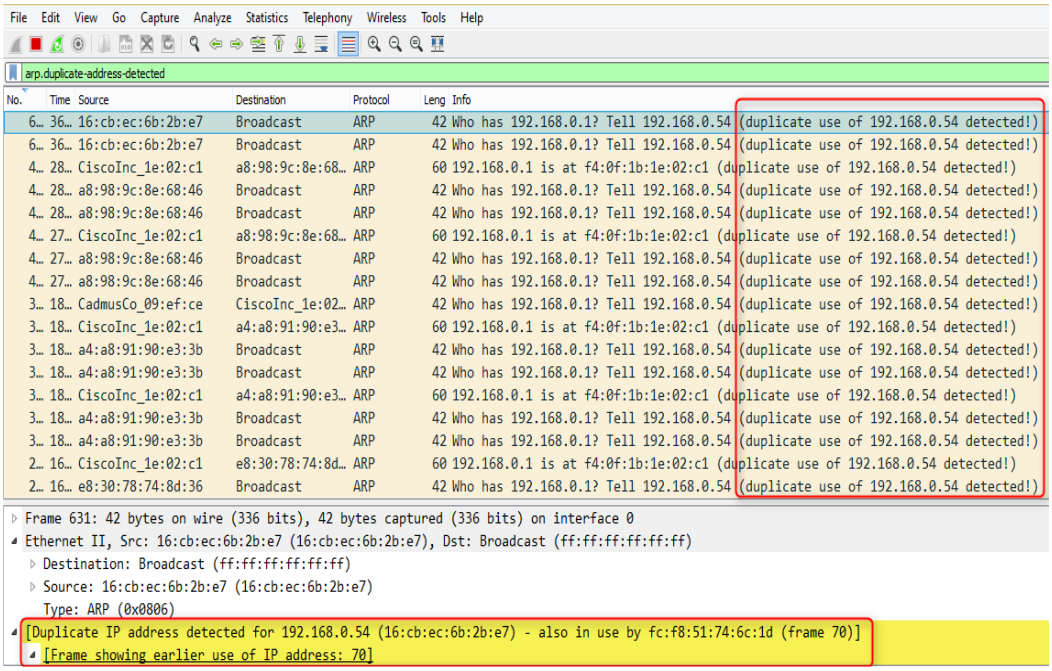

Figure 5. Analyzing traffic for ARP poisoning attempt.

2.2.8. Analyze traffic to detect malware activity

Evidence of a malware infection can be detected by analyzing the ongoing network traffic patterns. Malware often attempts to establish connections with Command-and-Control (C2) servers for activities such as data exfiltration or receiving further instructions. These connections involve specific IP addresses or opened ports on the infected system, which can be monitored using tools like Wireshark[21–23].

2.2.9. Identification of suspicious behavior

Example Scenario: In the provided example, attention is drawn to a specific communication attempt where IP address 10.10.10.12 is trying to connect to IP address 10.10.10.16 on port 1177 (**Figure 6**).

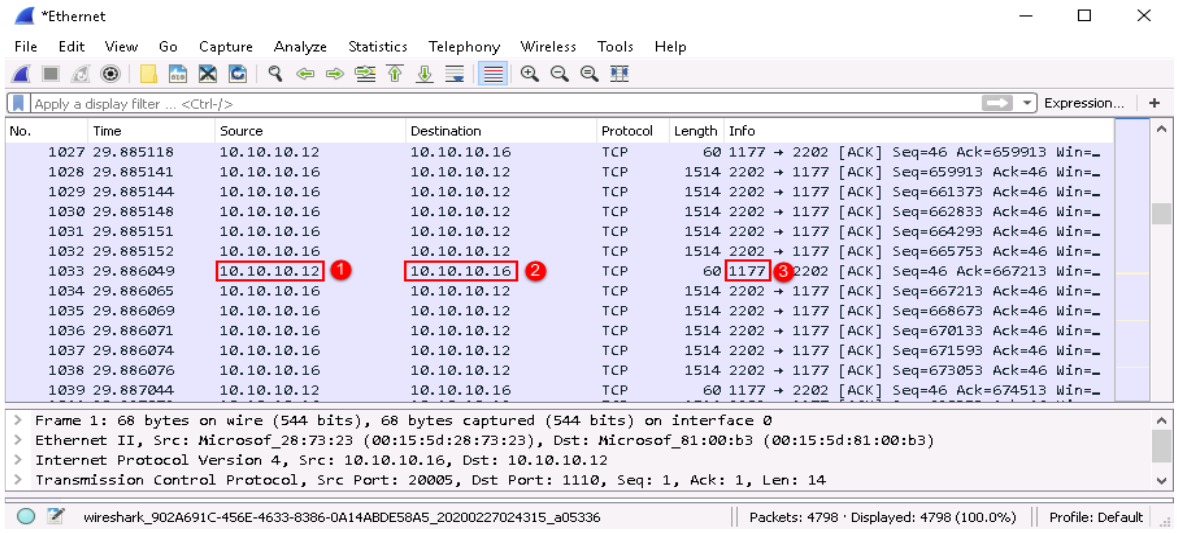

Figure 6. Observation of attempting to connect to IP 10.10.10.16 (1) on port 1177, which raises suspicions.

Raising Suspicions: This communication raises suspicions as it may indicate potentially malicious activity. Unusual ports or unexpected connections can be indicators of a security threat, such as malware attempting to communicate with a command-and-control server.

2.2.10. Verification through Internet databases

Searching for Known Malware Signatures: Once suspicious ports or IP addresses are identified, the recommendation is to conduct further investigation. This involves searching internet databases, specifically those that catalog known malware signatures and behaviors.

Example with njRAT Malware: In the given example, an internet search on speedguide.net's port database reveals that the njRAT malware is known to commonly employ port 1177 (**Figure 7**), as a default port[24].

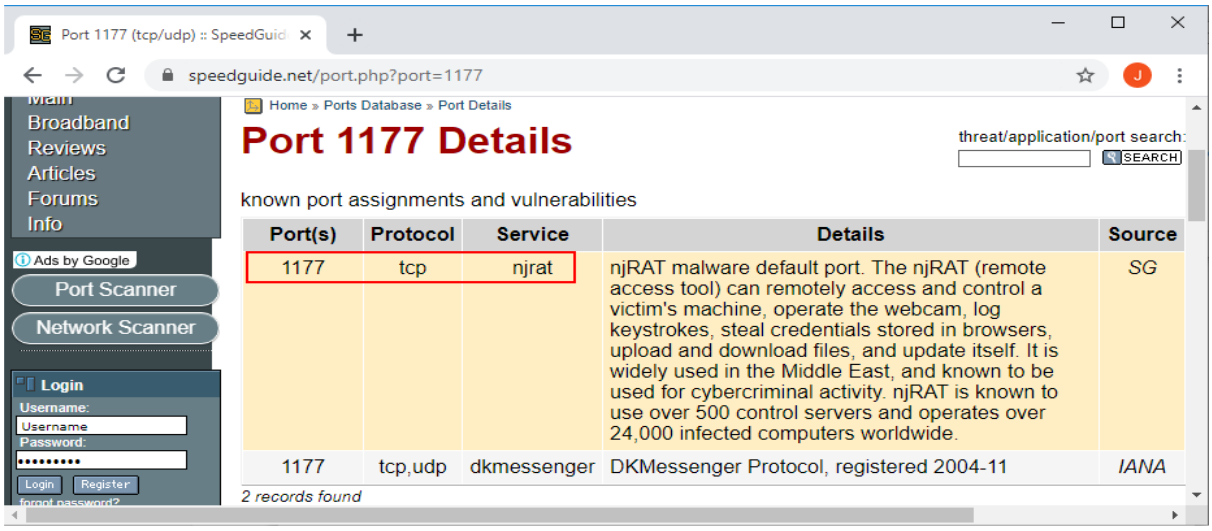

Figure 7. Uncovering speedguide.net's port database about the njRAT malware commonly employs port 1177 as a default port.

A comparative analysis of packet sniffers, specifically Tcpdump and Wireshark, alongside Security Information and Event Management (SIEM) systems can shed light on their respective strengths, weaknesses, and applications in the context of network forensics and security operations. Below is a breakdown of key aspects for such a comparison:

1) Scope and purpose

Tcpdump and Wireshark:

Scope: Primarily packet sniffers, focused on capturing and analyzing network traffic. Purpose: Provide detailed packet-level insights for network troubleshooting and forensics.

SIEM Systems:

Scope: Comprehensive security platforms designed to collect, correlate, and analyze log and event data from diverse sources. Purpose: Offer a holistic view of security events, enabling threat detection, incident response, and compliance management.

2) Ease of use

Tcpdump and Wireshark:

Ease: More technical and command-line driven, requiring expertise in networking protocols. User Interface: Wireshark offers a graphical user interface (GUI) for easier navigation.

SIEM Systems:

Ease: Typically user-friendly with GUIs, making them accessible to security analysts with varying technical backgrounds.

3) Data collection

Tcpdump and Wireshark:

Data Source: Capture raw network packets. Granularity: High level of granularity at the packet level.

SIEM Systems:

Data Source: Collect logs and events from various sources, including network devices, servers, and applications. Granularity: Aggregates data for a broader view of security events.

4) Analysis and correlation

Tcpdump and Wireshark:

Analysis: Deep packet inspection for forensic analysis. Correlation: Limited correlation capabilities.

SIEM Systems:

Analysis: Correlates data from multiple sources to identify patterns and anomalies. Correlation: Advanced correlation capabilities to detect complex security incidents.

5) Real-time monitoring

Tcpdump and Wireshark:

Real-Time: Can capture and analyze in real-time but with potential performance impacts.

SIEM Systems:

Real-Time: Designed for real-time monitoring and alerting.

6) Use cases

Tcpdump and Wireshark:

Use Cases: Network troubleshooting, packet-level forensics.

SIEM Systems:

Use Cases: Threat detection, incident response, compliance management.

7) Scalability

Tcpdump and Wireshark:

Scalability: Limited scalability for large-scale networks.

SIEM Systems*:*

Scalability: Designed to handle large-scale environments with distributed architectures.

8) Cost

Tcpdump and Wireshark:

Cost: Open-source and generally free.

SIEM Systems:

Cost: Can be expensive, often involves licensing fees.

Tcpdump and Wireshark excel in detailed packet-level analysis and troubleshooting, whereas SIEM systems provide a broader and more holistic approach to security by correlating data from diverse sources. The choice between them depends on the specific needs, technical expertise, and the scale of the network environment. For comprehensive security operations, a combination of both packet sniffers and SIEM systems may be ideal.

3. Results

The primary aim of the conducted research was to successfully gather and analyze network-based evidence, and this objective was effectively achieved. To achieve this, a range of network monitoring tools, including tcpdump and Wireshark, were employed. These tools play a crucial role in intercepting and recording network traffic, providing a wealth of data that can be subjected to in-depth analysis.

Tcpdump and Wireshark are renowned for their ability to capture and record packets of data traversing a network. They allow for the detailed examination of network communications, making them invaluable in the context of cybersecurity and digital forensics. By using these tools, the research was able to collect a comprehensive dataset of network traffic, which served as the foundation for the subsequent analysis.

Furthermore, the research harnessed the power of a Security Information and Event Management system (SIEM). SIEM systems are widely employed by large enterprises to efficiently manage and analyze security-related events and data. They excel in sifting through vast volumes of system logs and generating comprehensive reports on potential security threats or incidents. In the research context, the SIEM system played a pivotal role in automating the initial stages of data processing and helped in the efficient categorization of security events and incidents.

The analysis phase of the research was a critical step that involved a meticulous examination of the collected evidence for various types of network-based attacks and malicious activities. These activities included the identification of Sniffing Attempts, where unauthorized access to network traffic was detected, MAC Flooding Attempts, which involved attempts to overload network switches, FTP Password Cracking Attempts, which indicated efforts to gain unauthorized access to FTP servers, ARP Poisoning Attempts, a technique used to manipulate network traffic, and the detection of Malware Activity, which signified the presence of malicious software on the network.

This comprehensive analysis aimed to uncover patterns, anomalies, and potential indicators of malicious intent within the network data. Identifying these patterns and activities is crucial for enhancing network security, preventing data breaches, and responding effectively to cyber threats.

In summary, the research successfully achieved its primary objective by gathering and analyzing network-based evidence using tools like tcpdump, Wireshark, and a SIEM system. The analysis phase was particularly focused on detecting various network-based attacks and malicious activities, contributing to the broader goal of bolstering cybersecurity measures and safeguarding digital assets.

4. Discussion

The research conducted a meticulous examination of network traffic and conducted in-depth analysis with the overarching objective of identifying any indications of unauthorized access, suspicious behaviors, or potential security breaches within the network environment. This approach was designed to provide a comprehensive understanding of network vulnerabilities and to strengthen the overall resilience of the network infrastructure against future cyber threats.

Thoroughly examining network traffic is a fundamental step in cybersecurity and digital forensics. It involves scrutinizing the data packets that traverse the network, which can carry valuable insights into the activities and interactions occurring within the network. The analysis process delves deep into the characteristics of network traffic, including the origins and destinations of data packets, the protocols and services being utilized, and the volume and frequency of data transfers.

One primary focus of this examination is to detect any signs of unauthorized access. Unauthorized access refers to attempts by individuals or entities to gain entry to network resources, systems, or data without proper authorization. By scrutinizing network traffic patterns and access logs, the research sought to identify unusual

login attempts, access requests to restricted areas, or any anomalous behaviors indicative of unauthorized access. Such findings can be critical in preventing security breaches and protecting sensitive information.

Additionally, the research aimed to uncover suspicious behaviors within the network. Suspicious behaviors can encompass a wide range of activities that may not be explicitly unauthorized but could still pose security risks. These behaviors may include unusual data transfers, unexpected changes in user behavior, or patterns that deviate from established norms. Detecting and analyzing these behaviors can help security teams proactively identify potential threats before they escalate into full-blown security incidents.

Furthermore, the research was geared toward identifying potential security breaches. Security breaches involve successful unauthorized access or malicious activities that compromise the confidentiality, integrity, or availability of network resources. By scrutinizing network traffic for signs of security breaches, such as data exfiltration attempts, malware propagation, or exploitation of vulnerabilities, the research aimed to prevent or mitigate the impact of such incidents.

The comprehensive approach taken in this research not only serves the purpose of identifying immediate security threats but also contributes to the broader goal of fortifying the network infrastructure against future attacks. Understanding network vulnerabilities and areas of weakness allows organizations to implement proactive security measures, such as patching vulnerabilities, enhancing access controls, and deploying intrusion detection systems. By gaining insights into the tactics, techniques, and procedures employed by potential adversaries, organizations can better prepare and defend against evolving cyber threats.

In conclusion, the research's thorough examination of network traffic and in-depth analysis aimed to uncover unauthorized access, suspicious behaviors, and potential security breaches within the network environment. This comprehensive approach not only enhances immediate threat detection but also provides valuable insights for strengthening network security and resilience against future attacks, ultimately safeguarding digital assets and ensuring the integrity of network infrastructure.

Future research

Expanding the discussion on potential future research directions in the field of network forensics is crucial for keeping the paper current and guiding readers toward areas that may benefit from further exploration and innovation. Below are some considerations to enhance this section:

Emerging technologies:

5G Networks: Investigate the unique challenges and opportunities posed by the increasing adoption of 5G networks, exploring how the characteristics of these networks impact forensic practices.

IoT Security: Delve into the forensic implications of the growing Internet of Things (IoT), considering the unique challenges associated with investigating devices that may have limited resources.

Advanced attack vectors:

AI and Machine Learning Attacks: Explore the forensic challenges posed by attacks leveraging artificial intelligence and machine learning, emphasizing the need for new methodologies to detect and investigate these sophisticated threats.

Quantum Computing Threats: Anticipate the impact of quantum computing on encryption and investigate how this will influence forensic practices in a post-quantum cryptography era.

Integration of blockchain:

Blockchain Forensics: Investigate the forensic challenges and opportunities presented by blockchain technologies, exploring methods for tracing transactions on decentralized ledgers.

Enhanced data visualization:

Visual Analytics: Explore advanced data visualization techniques to present forensic findings in more intuitive and informative ways, aiding investigators in quickly identifying patterns and anomalies.

Automation and orchestration:

Automated Forensic Tools: Investigate the development of automated forensic tools and orchestration frameworks that can streamline and enhance the efficiency of the forensic process.

Legal and ethical considerations:

Global Legal Standards: Investigate the potential for establishing global standards for legal and ethical considerations in network forensics to harmonize practices across jurisdictions.

Privacy-preserving techniques:

Privacy-Enhancing Technologies: Explore methods to conduct effective network forensics while respecting user privacy, including the development of privacy-preserving techniques and protocols.

Collaborative forensics:

Cross-Organization Collaboration: Investigate models for collaborative network forensics, enabling different organizations to share information and collaborate effectively in incident response.

Human factors in forensics:

Human-Centric Approaches: Explore how human factors, such as cognitive biases and decision-making processes, impact the effectiveness of network forensic investigations.

Continuous evaluation of methodologies:

Methodology Validation: Encourage ongoing evaluation and validation of existing forensic methodologies to ensure they remain effective in the face of evolving technologies and attack vectors. By providing a roadmap for potential future research directions, the paper can contribute to the advancement of the field of network forensics and inspire researchers and practitioners to address emerging challenges and opportunities.

5. Conclusion

The realm of network forensics demands a holistic approach that intertwines technical proficiency with a keen awareness of legal considerations. Security Information and Event Management (SIEM) systems emerge as indispensable assets, empowering Computer Security Incident Response Teams (CSIRTs) to adeptly collect and monitor network data. Nevertheless, the formidable challenge posed by the sheer volume of data in network forensics necessitates a systematic methodology. This research underscores the significance of establishing legal boundaries and presenting evidence in an organized manner, emphasizing the crucial interplay between technical and legal expertise. By advocating for a systematic approach that prioritizes relevant evidence and adheres to legal and ethical standards, this study aims to provide CSIRTs with a comprehensive framework. This framework is designed to enhance the effectiveness of network evidence collection and analysis, allowing CSIRTs to navigate the intricate legal landscape while harnessing the wealth of network data for investigative purposes.

Author contributions

Conceptualization, DK; methodology, DK; validation, MB; formal analysis, DK; investigation, DK; resources, SR, AS and PS; data curation, MB; writing—original draft preparation, DK; writing—review and editing, DK; visualization, SR, AS and PS; supervision, MB; project administration, MB. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. He J, Chang C, He P, et al. Network Forensics Method Based on Evidence Graph and Vulnerability, MDPI, 2022. 8(4): 1–18.
2. Qureshi S, Tunio S, Akhtar F, et al. Network Forensics: A Comprehensive Review of Tools and Techniques. (IJACSA) International Journal of Advanced Computer Science and Applications, 2021. 12(5): 879–887.
3. Paxton N, Gail-Joon A, Chu B. Towards Practical Framework for Collecting and Analyzing Network-Centric Attacks, 2021 IEEE International Conference on Information Reuse and Integration, 2021.
4. Cheng BC, Chen H. Quality Assurance for Evidence Collection in Network Forensics, Information Security Applications. 7th International Workshop, WISA 2020, 2020.
5. Ping Y. Study on the main form of network crime from the view of criminology. 2021 International Conference on Human Health and Biomedical Engineering. Jilin, China. 2021.
6. Jayasingh BB, Patra MR. Rule Based Evidence Mining for Network Attack. 10th International Conference on Information Technology, 2019.
7. Kim HS, Kim HK. Network Forensic Evidence Acquisition (NFEA) with Packet Marking. Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, 2020.
8. Castiglione A, Cattaneo G, De Maio G. Forensically-Sound Methods to Collect Live Network Evidence. 2019 IEEE 27th International Conference on Advanced Information Networking and Applications, 2019.
9. Turnbull B, Slay J. Member, Wi-Fi Network Signals as a Source of Digital Evidence: Wireless Network Forensics. The Third International Conference on Availability, Reliability and Security, 2022.
10. Kim DH. Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics. 2022 International Conference on Information Security and Assurance, 2022, 193–198. doi: 10.1109/ISA.2008.90.
11. Volarević M, Tomić L. Milohanić, Network forensics, 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), 2022, pp.1025–1030.
12. Zhang R, Xie M, Bian J. ReLF: Scalable Remote Live Forensics for Android, 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2021, pp. 822–831.
13. Nehinbe JO, Damuut P. Security issues in Sensor Networks and gathering admissible evidence in Network Forensics, 2021 UKSim 5th European Symposium on Computer Modeling and Simulation, 2021.
14. Masys A. Networks and network analysis for defence and security, 2022 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2022
15. Kumar M, Hanumanthappa M, Suresh Kumar TV. Crime investigation and criminal network analysis using archive call detail records, 2019 IEEE Eighth International Conference on Advanced Computing (ICoAC), 2019.
16. Liu Y, Chen G, Xie L. An Email Forensics Analysis Method Based on Social Network Analysis, 2020 International Conference on Cloud Computing and Big Data, 2020.
17. Tian Z, Jiang W, Li Y, Dong L. A digital evidence fusion method in network forensics systems with Dempster-Shafer theory, China Communications, 2022. 11(5): 91–97.
18. Wright P, Fone W. Designing and Managing Networks to Aid the Capture and Preservation of Evidence to support the Fight Against e-Crime, Proceedings of the 2021 IEEE International Conference on MonM04; Networking, Sensing and Control. April 2021; London, UK. pp. 15–17.
19. Amato F, Cozzolino G, Mazzeo A, Mazzocca N. Correlation of Digital Evidences in Forensic Investigation through Semantic Technologies, 2020 31st International Conference on Advanced Information Networking and Applications Workshops, 2020.
20. Zainudin NM, Merabti M, Llewellyn-Jones D. Online social networks as supporting evidence: A digital forensic investigation model and its application design. Available online: https://ieeexplore.ieee.org/document/6125728 (accessed on 23 May 2023).
21. Liu C, Singhal A, Wijesekera D. A logic-based network forensic model for evidence analysis. IFIP International Conference on Digital Forensics, 2021.
22. Network-Based Evidence. Indian law portal. Available online: https://indianlawportal.co.in/network-based-evidence/ (accessed on 26 May 2023).
23. Saravanany P, Sethukkarasi T. Network Forensics: An Analysis of Techniques, Tools and Trends, IEEE Xplore Computers, 2020.
24. Network Evidence Collection. Available online: https://www.packt.com/network-evidence-collection/ (accessed on 28 May 2023).